UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/787,029	03/13/2001	Takuya Hirano	010294	8139

38834 7590 08/24/2005

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP
1250 CONNECTICUT AVENUE, NW
SUITE 700
WASHINGTON, DC 20036

EXAMINER	
PICH, PONNOREAY	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 08/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/787,029	HIRANO, TAKUYA	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 July 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim 1 was amended. Claims 15-24 were newly added. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action. The previous office action(s) is/are incorporated by reference in its/their entirety. The examiner assumes that the applicant agrees with any well-known prior art statements and/or rejections made by the examiner in the previous office action(s) that were not argued. Any objections or rejections not repeated below for record are withdrawn due to applicant's amendments and/or arguments.

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 7/21/2005 has been entered.

Docketing

Please note that the application has been redocketed to a different examiner. Please refer all future communications regarding this application to the examiner of record using the information supplied in the final section of the office action.

Specification

Applicant is reminded of the proper content of an abstract of the disclosure.

A patent abstract is a concise statement of the technical disclosure of the patent and should include that which is new in the art to which the invention pertains. If the patent is of a basic nature, the entire technical disclosure may be new in the art, and the abstract should be directed to the entire disclosure. If the patent is in the nature of an

improvement in an old apparatus, process, product, or composition, the abstract should include the technical disclosure of the improvement. In certain patents, particularly those for compounds and compositions, wherein the process for making and/or the use thereof are not obvious, the abstract should set forth a process for making and/or use thereof. If the new technical disclosure involves modifications or alternatives, the abstract should mention by way of example the preferred modification or alternative.

The abstract should not refer to purported merits or speculative applications of the invention and should not compare the invention with the prior art.

Where applicable, the abstract should include the following:
(1) if a machine or apparatus, its organization and operation;
(2) if an article, its method of making;
(3) if a chemical compound, its identity and use;
(4) if a mixture, its ingredients;
(5) if a process, the steps.

Extensive mechanical and design details of apparatus should not be given.

The abstract in the second paragraph makes a statement concerning the purported merits or speculative application of the invention.

Claim Objections

Claims 1, 3, 6, and 15-17 are objected to because of the following informalities:

1. As per claim 1, the examiner submits in that line 4 should be an "a" before "privacy key", i.e. "a signal of **a** privacy key".
2. As per claim 3, the examiner submits that there should be a comma after "lights" in the last line of the claim.
3. As per claim 6, the examiner submits that applicant may have meant to recite "...through **a** longer one of two..." on line 4 and lines 19-20.
4. As per claim 6, the examiner submits that on lines 11 and 18, applicant may have meant to recite "...through **a** shorter one of two...."

5. As per claim 6, lines 25-26, the examiner submits that applicant may have meant to recite "an amplifier for amplifying a difference signal, representative of a difference between said two output lights, to output an amplified corresponding voltage." Note the commas.
6. As per claims 15-17, they currently recite in several places "as a raw key for candidate being adopted as a privacy key." The examiner submits that perhaps applicant meant to recite "as a raw key candidate for being adopted as a privacy key" or "as a raw key candidate to be adopted as a privacy key."
7. As per claims 15-17, in the last line of each claim, the examiner submits that perhaps applicant meant to recite "said threshold value +X or –X." Note the "or" instead of an "and".

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-24 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1. Claim 1 refers to an "optical balanced homodyne detector". Such a detector is not disclosed in the specification.

2. Claim 1 recites "said phase difference" and "the phase difference." It is unclear if both terminologies refer to the same phase difference first recited in line 3.
3. Claim 1 recites "the detector" in line 7, which lacks antecedent basis.
4. Claim 2 recites in line 6, "said reference signal" and "said transmission signal" which lacks antecedent basis.
5. Claim 3 recites on lines 7-8 "said system", which lacks antecedent basis.
6. As per claim 3, it is unclear what is operative (as recited in line 8) after a relative phase difference is imparted between said transmission and reference signals.
7. Claim 3 recites, "said phase-modulated weak transmission signal" and "said phase modulated intense reference signal" which lacks antecedent basis.
8. Claim 5 recites, "said reference signal" and "said transmission signal" which lacks antecedent basis as not every claim in claims 1-4 from which claim 5 depends recites "said reference signal" and "said transmission signal", i.e. see claim 1.
9. As per claim 5, the examiner respectfully submits that the phrasing of "...and as polarized..." in the claim seems worded incorrectly or misplaced in the limitation. The examiner assumes that applicant may have meant "...and are polarized...."
10. Claim 6 recites in lines 8-9 "said transmission signal" which lacks antecedent basis.
11. Claim 6 recites in line 10 "said intense reference signal" which lacks antecedent basis.
12. Claim 6 recites "the received signal" on lines 11-12, which lacks antecedent basis.

13. Claim 6 recites on line 12 "said system" which lacks antecedent basis.

14. As per claim 6, it is unclear what is operative (as recited in line 12) after a relative phase difference is imparted.

15. Claim 6 recites on line 19, "said isolated reference signal" which lacks antecedent basis.

16. Claim 7 recites in line 2, "said optical fiber" which lacks antecedent basis.

17. Claim 8 recites "said transmission signal" and "said threshold values" which lacks antecedent basis as not every claim in claims 1-4, 6, or 7 from which claim 8 depends recites antecedent basis "said transmission signal" and "said threshold values", i.e. see claim 1.

18. Claim 9 recites "the phase modulations", "said reference signal" and "said transmission signal" which lacks antecedent basis as not every claim in claims 1-4, 6, or 7 from which claim 9 depends recites antecedent basis for "the phase modulations", "said reference signal" and "said transmission signal", i.e. see claim 1.

19. Claim 10 recites "such phase modulations." It is not always clear in claims 1-4, 6, or 7 from which claim 10 depends to which phase modulations is being referred, i.e. see claim 1.

20. Claim 10 recites "those" in two separate instances in line 3. It is unclear to what "those" refers.

21. Claim 11 recites in line 3, "the error rate", which lacks antecedent basis.

22. Claim 13 recites "said two output lights" which lacks antecedent basis.

23. Claim 14 recites "said photoconductor diodes" which lacks antecedent basis.

24. Claim 15 recites on line 17 "said modulation means" which lacks antecedent basis.

25. Claim 15 recites "the total phase difference" on line 31 which lacks antecedent basis.

26. Claim 15 recites "the signal light" and "the reference light" in lines 31-32. It is unclear of these lights refer to the same light which were earlier referred to as "said signal light" and "said reference light", i.e. see line 10.

27. Claim 15 recites "the phase change notified by the recipient" and "the phase change imparted by the sender" in lines 31-32 which lacks antecedent basis.

28. Claim 15 recites in line 33 "the lights" which lacks antecedent basis.

29. As per claim 15, the limitation recited in lines 40-42 seems worded incorrectly, i.e. "for said every light making notified as a raw key for candidate...."

30. Claim 16 recites "said every signal light" on line 23, which lacks antecedent basis.

31. Claim 16 recites "said every reference light" on line 25, which lacks antecedent basis.

32. Claim 16 recites "the signal light" and "the reference light" in lines 29-30. It is unclear of these lights refer to the same light which were earlier referred to as "said signal light" and "said reference light", i.e. see lines 10-11.

33. Claim 16 recites "said phase change notified by the recipient" and "said phase change imparted by the sender" in lines 30-31 which lacks antecedent basis.

34. Claim 16 recites "the lights" in line 31 which lacks antecedent basis.

35. As per claim 16, the limitation recited in lines 38-41 seems worded incorrectly, i.e. "for said every light making notified as a raw key for candidate...."

36. Claim 17 recites "said polarizations" in line 21-22 which lacks antecedent basis.

37. Claim 17 starting at line 38 recites limitations similar to what is found in claim 16 and contains similar 112, second paragraph problems as the ones mentioned above for claim 16.

38. Claim 17 recites on line 11, "a phase modulator for changing the phase of said signal light and mirrors." It is unclear how a phase modulator would change the phase of a mirror which has no phase angle. It is noted, however, that a mirror can be adjusted to modulate the phase angle of light waves.

39. Claim 17 recites "the short optical path", "said short optical path", "the long optical path", and "said long optical path". It is unclear if "the short optical path" and "said short optical path refers to the same short optical path and if "the long optical path" and "said long optical path" refers to the same long optical path.

40. Claim 18 recites "said single mode optical fiber" and "said reference signal" which lacks antecedent basis.

41. Claim 19 recites "said reference signal" and "said transmission signal" which lacks antecedent basis.

42. Claim 21 recites "the error rate" which lacks antecedent basis.

43. Claim 23 recites "said photoconductor diodes" which lacks antecedent basis.

44. Claim 24 recites "the said signal light which lacks antecedent basis.

45. Claim 24 recites "said reference light" and is dependent on claims 15-17. It is unclear if "said reference light" is meant to refer to the same reference light as "the reference light" recited in some of the claims that claim 24 is dependent, i.e. see claim 15.

46. Claim 24 recites "a single photon or so." It is unclear how many photons are encompassed by "or so."

47. Any claims not specifically addressed are rejected by virtue of dependency.

48. Appropriate corrections are required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Townsend (US 5,675,648) in view of Werner et al ("Eavesdropping using quantum-nondemolition measurements").

Claim 1:

Townsend discloses in a quantum cipher communication using a light signal, a quantum cipher communication system characterized in that:

1. It uses a phase difference between a signal light and a reference light which have orthogonal polarizations for a signal of a privacy key, wherein said phase

difference is produced by a sender and a recipient adding a phase on the signal light or the reference light (col 3, lines 26-45).

2. Wherein an eavesdropping is detected by the recipient measuring a change in a quantum-mechanical probability distributions of said difference signal, which is produced by the eavesdropping operation (col 3, lines 56-64).

Townsend does not disclose "it has an optical balanced homodyne detector which detects said phase difference as a difference signal of the detector, wherein the phase difference is determined by comparing said difference signal with a threshold voltage." However, the examiner submits that the limitation is well known in the art. Further, the limitation is disclosed by Werner (p640, Figure 1a).

In light of the above, it would have been obvious to one of ordinary skill in the art to use Warner's teachings to modify Townsend's invention according to the limitations recited in claim 1. One of ordinary skill would have been motivated to do so as homodyne detectors offer the best receiver sensitivity among all binary signaling techniques employing single-bit decisions. This would increase Townsend's likelihood of detecting an eavesdropper.

Claims 2, 5, 8-11, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Townsend (US 5,675,648) in view of Werner et al ("Eavesdropping

using quantum-nondemolition measurements") and further in view of Bethune et al (US 6,188,768).

Claim 2:

As per claim 2, Townsend and Werner meet all the limitations except the following limitations, which is met by Bethune.

Bethune meets the limitation of "splitting a light signal from a transmission source side into an intense reference signal and a weak transmission signal which is so weak that a change in its quantum mechanical state is detectable" on column 2, lines 28-37; and "imparting a phase difference between said reference signal and said transmission signal while they are in a process of transmission" on column 2, lines 28-37. They are orthogonally polarized and hence are imparted a specific phase difference. Bethune meets the limitation of "superimposing in a transmission receiving side said reference signal and said transmission signal to form two output lights which are opposite in phase and producing a difference signal which is represented by a difference between said two output lights" on column 2, lines 28-37; and the limitation "deriving a frequency distribution of said difference signal as a function of a fluctuation of the quantum state of said transmission signal based upon or in accordance with the frequency distribution of said difference signal, making privacy (secret) keys respectively at said transmission source and receiving sides or holding in common thereby" is made obvious on column 2, lines 51-57 and abstract, last sentence. The key after being decoded is communicated to the other receiving party. Bethune meets the limitation of "directly

observing the fluctuation of the quantum state of said transmission signal" on column 2, lines 51-57 and column 5, lines 61-64.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bethune within the combination invention of Townsend and Werner so as to enable a secure key distribution system between two parties.

Claim 5:

With respect to Claim 5, all the limitations are met by Townsend and Werner except for the following limitation.

Bethune meets the limitation of "characterized in that said reference signal and said transmission signal are split both in time and as polarized and then transmitted to travel along a common path" in the abstract.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bethune within the combination invention of Townsend and Werner as to enable a secure key distribution system between two parties.

Claim 8:

With respect to Claim 8, Townsend and Werner meet all the limitations except the following limitation. The limitation of "characterized in that threshold values are established, respectively, for positive and negative values of said difference signal, and that the state of said transmission signal is discriminated on the basis of said threshold values" by Bethune on column 7, lines 32-46.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bethune within the combination invention of Townsend and Werner so as to enable a secure key distribution system between two parties.

Claim 9:

With respect to Claim 9, all the limitations are met by Townsend and Werner except the following limitation. The limitation of "characterized in that in addition to the phase modulations designed to transmit privacy keys, such a phase modulation is so imparted as described and having a value later determined for making a correction for a fluctuation of the difference in optical path between said reference signal and said transmission signal which develops by reason of an external cause" is met by Bethune on column 7, lines 32-46.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bethune within the combination invention of Townsend and Werner because the fluctuation in the difference signal by an external cause determines if an eavesdropper has gained access to the communication.

Claim 10:

With respect to Claim 10, all the limitations are met by Townsend and Werner except the following limitation.

The limitation of "characterized in that such phase modulations are so imparted as described and including those for transmitting privacy keys and those with values later determined are randomly repeated" is met by Bethune on column 6, lines 6-28. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bethune within the combination invention of Townsend and Werner because introducing a randomness into the transmission process for key generation makes the generated key harder to guess by an attacker.

Claim 11:

With respect to Claim 11, all the limitations are met by Townsend and Werner except the following limitation.

The limitation of "characterized in that eavesdropping is detected on the basis of an increase in the error rate of said difference signal" is met by Bethune on column 5, lines 64-67 and on column 6, lines 1-5.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bethune within the combination invention of Townsend and Werner because detection of an eavesdropper allows the user to know that the keys are no longer secure and are to be discarded.

Claim 13:

With respect to Claim 13, all the limitation is met by Townsend and Werner except the following limitation.

The limitation of "characterized in that said two output lights are converted into corresponding electric signals through photoconductor diodes" is obvious over Bethune, Fig. 3A and 3B.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bethune within the combination invention of Townsend and Werner because conversion of the light signal to an electric signals allows the system to be able to measure the difference signal so as to decipher if the signal has been eavesdropped.

Claims 3-4 and 6-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bethune (6188768 B1).

Claim 3:

With respect to Claim 3, Bethune meets the limitation of "a first beam splitter for splitting a light from a light source into a transmission signal and a reference signal" on column 2, line 67 and column 3, lines 1-2. The light is split into two signals and because these signals are polarized orthogonally, this makes splitting of the beams into a transmission and a reference signal obvious. Bethune meets further limitation of "a phase modulating means for imparting a phase modulation to said transmission signal" on column 2, lines 63-67; and "a light attenuator for converting only said transmission signal into a weak transmission signal which is so weak that a change in its quantum state is detectable" on column 3, lines 47-67 (When P2 (the transmission signal) returns

to C2, only a portion of it is directed back to the laser and detector. This directed portion is obviously weaker than the entire P2 signal and it is then fed into a detector. The detector should then detect this change in its quantum mechanical state.

By scattering the light pulse, a weaker signal emerges. Further limitation of "a phase modulating means for imparting a phase modulation to said reference signal, said system also including, operative after a relative phase difference is imparted between said transmission and reference signals" is met in the abstract; and "a second beam splitter for superimposing said phase modulated weak transmission signal and said phase modulated intense reference signal to form two output lights" on column 5, lines 32-41. PBS1 and PBS2 are the two beam splitters. Bethune meets the limitation of "a first and a second photoelectric conversion elements for converting said two output lights from said second beam splitter into two corresponding electric signals which are opposite in phase" on column 6, lines 6-14; and "an amplifier for amplifying a difference signal representative of a difference between said two output lights to output an amplified corresponding voltage" on column 6, lines 20-28 and 1-5. The difference signal is represented by the combined signals. The amplifier is represented by the power meter monitor because it detects a difference in both signals and decides if the signal has been eavesdropped.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have an amplifier present in the invention because the presence of an amplifier within the power meter monitor will amplify the difference signal so that the signal can be accurately measured to determine if it has been eavesdropped.

Claim 4:

With respect to Claim 4, Bethune meets the limitation of "characterized in that said phase modulating means includes a mirror movable by a distance as small as the wave length of an incident light" on column 1, lines 43-53, column 2,lines 5-12 and 58-63.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the Faraday mirror be adjustable by the distance as small as the wavelength of an incident light because this would enable the mirror be able to polarize the light pulse as accurately as it does. The faraday mirror introduces a change in phase of the light pulse.

Claim 6:

With respect to Claim 6, Bethune meets the limitation of "a first beam splitter for splitting a light from a light source into a transmission signal and a reference signal" on column 2, line 67 and column 3,lines 1-2; and "a first light polarizes for polarizing said transmission signal through longer one of two distance paths" on column 2, lines 37-42, 45-48 and 51-57; and "a light attenuator for converting only said transmission signal into a weak transmission signal which is so weak that a change in its quantum state is detectable" on column 3, lines 47-67. When P2 (the transmission signal) returns to C2, only a portion of it is directed back to the laser and detector. This directed portion is obviously weaker than the entire P2 signal and it is then fed into a detector. The detector should then detect this change in its quantum mechanical state. The scattering of the light pulse inherently weakens it. Bethune meets further limitation of "a first phase modulating means for imparting a predetermined phase modulation to said

transmission signal and a first polarized beam splitter for receiving said intense reference signal having passed through shorter one of two distance paths and said transmission, signal and returning the received signal to travel along a common optical path, said system also including, operative after a relative phase difference is imparted between said transmission and reference signals and included in a transmission receiving side" on column 5, lines 32-44; and "a second polarized beam splitter for isolating from each other said transmission and reference signals transmitted through a single optical fiber" on column 5, lines 32-33; and "a second phase modulating means for imparting a phase modulation to said isolated transmission signal through shorter one of two distance paths" on column 2, lines 42-48; and "a second light polarizer for polarizing said isolated reference signal through longer one of two distance paths" on column 5, lines 32-41; and "said system further including a second beam splitter for superimposing said transmission and reference signals which are coincident with each other in time and polarization to produce two output lights" on column 4, lines 53-54 and column 5, lines 32-41. PBS2 is the second beamsplitter. Further limitation of "a first and a second photoelectric conversion elements for converting said two output lights into corresponding electric signals which are opposite in phase" is met on column 6, lines 6-14; and "an amplifier for amplifying a difference signal representative of a difference between said two output lights to output an amplified corresponding voltage" is met on column 6, lines 20-28 and 1-5. The difference signal is represented by the combined signals. The amplifier is represented by the power meter monitor because it detects a difference in both signals and decides if the signal has been eavesdropped.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have an amplifier present in the invention because the presence of an amplifier within the power meter monitor will amplify the difference signal so that the signal can be accurately measured to determine if it has been eavesdropped.

Claim 7:

With respect to Claim 7, Bethune meets the limitation of "characterized in that a third light polarizes is provided in an output side of said optical fiber for making a correction for a disturbance of polarization of said reference signal" on column 5, lines 32-38.

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Townsend (US 5,675,648) in view of Werner et al (Eavesdropping using quantum-non demolition measurements) in and further in view of Bartelt et al (The Wigner Distribution Function—An Alternative Signal Representation in Optics).

Claim 12:

With respect to Claim 12, all the limitations are met by Townsend and Werner except for the following limitation.

The limitation of "characterized in that eavesdropping is detected on the basis of a change in a Wigner distribution function that indicates a quantum mechanical state of said difference signal" is met by Bartelt on page 260.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bartelt et al within the system of Werner because the Wigner distribution function is an effective way to determine if the signal has been eavesdropped.

Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Townsend (US 5,675,648) in view of Werner et al ("Eavesdropping using quantum-nondemolition measurements") and further in view of Bethune et al (US 6,188,768) and Lee US 5,665,423).

Claim 14:

As per claim 14, all the limitations are met by Townsend, Werner, and Bethune except the following.

Lee meets the limitation of "characterized in that for said photoconductor diodes, use is made of silicon photoconductor diodes when the light has a wave length of 600 nm to 900 nm, and InGaAs photoconductor diodes when the light has a wave length of 1000 nm to 1500 nm" on column 1, lines 26-38.

It would have been obvious to one of ordinary skill in the art to have modified the combination invention of Townsend, Werner, and Bethune according to the limitations recited in claim 14. One of ordinary skill would have been motivated to do so because the frequency of photodetectors depends on the material used (see Lee, column 1, lines 26-27).

Claims 15-21 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bethune et al (US 6,188,768) in view of Mazourenko et al (US 6,272,224), herein referred to as Maz, in further view of Townsend (US 5,675,648).

Claim 15:

Bethune discloses in quantum cipher communication using a light signal, a quantum cipher communication system having a sender's apparatus, a recipient's apparatus and a transmission path connecting between the sender's apparatus and the recipient's apparatus (Fig 1-5), characterized in that

1. The sender's apparatus comprises of:
    a. A light source for a laser beam (col 2, lines 28-37).
    b. A beam splitting means for splitting said laser beam into a signal light and a reference light (col 2, lines 28-37).
    c. A phase modulation means making a phase change for every light which is either of said signal light or said reference light (col 2, lines 28-37).
    d. A light attenuation means for attenuating said signal light intensity (col 3, lines 47-67).
2. The recipient's apparatus comprises of:
    a. A phase modulation means making a phase change for every light which is either of said signal light or said reference light transmitted from the sender's apparatus through the transmission path (col 2, lines 42-48).

b. An amplifying means for amplifying a difference signal between said electric signals (col 6, lines 1-5 and 20-28).

3. Wherein the sender, by using said phase modulation means of sender's apparatus, imparts for every light a phase change randomly selected from a set of phase changes predetermined by the sender and the recipient, and the recipient, by using said phase modulation means of recipient's apparatus, imparts for every light a phase change randomly selected from said set of phase changes, as well as measures for every light said difference signal between the electric signals amplified by the amplifying means (col 7, lines 32-39).

Bethune does not disclose the recipient apparatus comprises of a superimposing means for superimposing said signal light and said reference light, either of which is phase changed by said modulation means of the recipient's apparatus and the recipient apparatus comprises a pair of photo-detector for converting two output lights into respective electronic signals.

However, Maz discloses the recipient apparatus comprises of a superimposing means for superimposing said signal light and said reference light, either of which is phase changed by said modulation means of the recipient's apparatus (Fig 4 and col 4, lines 1-14). Maz further discloses the recipient apparatus comprises a pair of photo-detector for converting two output lights into respective electronic signals (col 3, lines 19-24).

Bethune and Maz do not disclose:

1. By using a public communication line, the recipient notifies to the sender said phase changes imparted by the recipient for every light.
2. The sender calculates the total phase difference between the signal light and the reference light by adding the phase change notified by the recipient and the phase change imparted by the sender for every light, and notifies to the recipient the lights whose total phase difference satisfy a condition predetermined by the sender and the recipient, as a raw key candidate being adopted as a privacy key.
3. Then the recipient, for every light notified as a raw key candidate, assigns bit 1 when said difference signal measured is equal or greater than a predetermined threshold value +X, and assigns bit 0 when said difference signal measured is equal or less that the predetermined threshold value –X, whereby the recipient gets a privacy key.
4. The sender, for said every light making notified as a raw key for candidate, assigns bit 1 or 0 according to a condition regarding the total phase difference, which is predetermined by the sender and the recipient, whereby the sender gets a privacy key.
5. Wherein the sender and the recipient can get the privacy key in common with suitable effective detection efficiency and suitable error rate by selecting a threshold value +X and –X.

However, Townsend discloses a quantum key distribution system wherein a light signal is randomly phase modulated on the sender's end and a recipient to perform a

detection of the modulated signal phase shifts the signal again (col 3, lines 26-37). Further, Townsend discloses that after the completion of the quantum communication, the sender and receiver uses a public channel to discuss which photons were encoded and decoded using the same type of phase shift (col 2, lines 9-17 and col 3, lines 55-62). Townsend further discloses that the total phase shift (the sender's phase shift minus the receiver's phase shift) is a used to determine if the key bit of the photon is determined to be a 0 or a 1 (col 3, lines 37-45). Townsend further discloses that the procedure is completed by comparing the measurements for eavesdropper induced errors (col 3, lines 62-64). These teachings by Townsend read on the above limitations not met by Bethune and Maz.

In light of the above, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Bethune's invention using Maz and Townsend's teachings according to the limitations recited in claim 15. One of ordinary skill would have been motivated to use Maz's teachings because Maz discloses that his teachings would allow for quantum coding by optical phase with a constant delay between the emitter and receiver (col 4, lines 29-34). One of ordinary skill would have been motivated to incorporate Townsend's teachings because Townsend discloses that his teachings would allow one to maintain the quantum cannel effectively over far greater distances than would otherwise be possible (col 2, lines 6-8).

Claim 16:

Bethune discloses in quantum cipher communication using a light signal, a quantum cipher communication system having a sender's apparatus, a recipient's

apparatus and a transmission path connecting between the sender's apparatus and the recipient's apparatus (Fig 1-5), characterized in that

1. The sender's apparatus comprises of:
    a. A light source for a laser beam (col 2, lines 28-37).
    b. A beam splitter for splitting said laser beam into a signal light and a reference light (col 2, lines 28-37).
    c. A moveable mirror making a phase change for every said light signal (col 2, lines 28-37 and 63-67).
    d. A light attenuator for attenuating said signal light intensity (col 3, lines 47-67).
    e. The transmission path comprises a pair of paths for transmitting said light signal and said reference light respectively (Fig 2).
2. The recipient's apparatus comprises of:
    a. A moveable mirror making a phase change for every said reference light transmitted from the sender's apparatus through one of the path of transmission (col 2, lines 42-48).
    b. A charge sensitive amplifier for amplifying a difference signal between said electric signals (col 6, lines 1-5 and 20-28).

Bethune does not disclose the recipient's apparatus comprises of:

1. A beam splitter for superimposing said signal light transmitted from the sender's apparatus through the other path of transmission and said reference light phase changed by said moveable mirror of the recipient's apparatus.
2. A pair of photoconductive diodes for converting two output lights from said beam splitter into respective signals.

However, Maz discloses the recipient apparatus comprises of a beam splitter for superimposing said signal light transmitted form the sender's apparatus through the other path of transmission and said reference light phase changed by said moveable mirror of the recipient's apparatus (Fig 4 and col 4, lines 1-14). Maz further discloses the recipient apparatus comprises a pair of photo-detector for converting two output lights from said beam splitter into respective electronic signals (col 3, lines 19-24).

Bethune and Maz do not disclose:

1. Wherein the sender, by using said movable mirror of the sender's apparatus, randomly imparts phase changes 0, 90, 180, or 270 degrees fro said every signal light, and the recipient, by using said movable mirror of recipient's apparatus, randomly imparts phase change 0 or 90 degrees for said every reference light, as well as measures said difference signal between the electric signals amplified by the charge sensitive amplifier.
2. Then, by using a public communication line, the recipient notifies to the sender said phase changes imparted by the recipient whether it is 0 or 90 degrees for every reference light.

3. The sender calculates the total phase difference between the signal light and the reference light by adding said phase change notified by the recipient and said phase change imparted by the sender for every light, and notifies to the recipient the lights whose total phase difference is either 0 or 180 degrees, as a raw key for candidate being adopted as a privacy key.
4. Then the recipient, for every light notified as a raw key for candidate being adopted as a privacy key, assign bit 1 when said difference signal measured is equal or greater than a predetermined threshold value +X, and assigns bit 0 when said difference signal measured is equal or less than the predetermined threshold value –X, whereby the recipient gets a privacy key.
5. The sender, for every light making notified as a raw key for candidate being adopted as a privacy key, assigns bit 1 when the phase imparted by the sender is 0 or 90 degrees, and assigns bit 0 when the phase imparted by the sender is 180 or 270 degrees, whereby the sender gets the privacy key.
6. Wherein the sender and the recipient can get the privacy key in common with suitable effective detection efficiency and suitable error rate by selecting said threshold value +X and –X.

However, Townsend discloses a quantum key distribution system wherein a light signal is randomly phase modulated on the sender's end and a recipient to perform a detection of the modulated signal phase shifts the signal again (col 3, lines 26-37). Note the sender phase shifts by 0, $\pi/2$, π, $3\pi/2$ radians and the receiver phase shifts by

0 or $\pi/2$ radians. This is the same as 0, 90, 180, 270 degrees for the sender and 0 and 90 degrees for the recipient. Further, Townsend discloses that after the completion of the quantum communication, the sender and receiver uses a public channel to discuss which photons were encoded and decoded using the same type of phase shift (col 2, lines 9-17 and col 3, lines 55-62). Townsend further discloses that the total phase shift (the sender's phase shift minus the receiver's phase shift) is a used to determine if the key bit of the photon is determined to be a 0 or a 1 (col 3, lines 37-45). Townsend further discloses that the procedure is completed by comparing the measurements for eavesdropper induced errors (col 3, lines 62-64). These teachings by Townsend read on the above limitations not met by Bethune and Maz.

In light of the above, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Bethune's invention using Maz and Townsend's teachings according to the limitations recited in claim 16. One of ordinary skill would have been motivated to use Maz's teachings because Maz discloses that his teachings would allow for quantum coding by optical phase with a constant delay between the emitter and receiver (col 4, lines 29-34). One of ordinary skill would have been motivated to incorporate Townsend's teachings because Townsend discloses that his teachings would allow one to maintain the quantum cannel effectively over far greater distances than would otherwise be possible (col 2, lines 6-8).

Claim 17:

Bethune discloses in quantum cipher communication using a light signal, a quantum cipher communication system having a sender's apparatus, a recipient's

apparatus and a transmission path connecting between the sender's apparatus and the recipient's apparatus (Fig 1-5), characterized in that

1. The sender's apparatus comprises of:
    a. A light source for a pulsed light (col 2, lines 28-37).
    b. A beam splitter for splitting said pulsed light into a signal light and a reference light (col 2, lines 28-37).
    c. A light attenuator for attenuating said signal light intensity (col 3, lines 47-67), a phase modulator for changing the phase of said signal light and mirrors (col 2, lines 28-37).
    d. A first polarized beam splitter for returning said signal light transmitted through said long optical path and said reference light onto a common optical axis, wherein said signal light and said reference light returned to the common optical axis have a mutual time delay based on the optical path length difference between said long optical path for the signal light and a short optical path where said reference signal reaches to the first polarized beam splitter from the beam splitter, and have mutually orthogonal polarizations (col 5, lines 13-25).
2. The recipient's apparatus comprises of:
    a. A second polarized beam splitter for splitting said signal light and said reference light transmitted through the single mode optical fiber (col 6, lines 6-19).

b. An amplifier for amplifying a difference signal between said electric signals (col 6, lines 1-5 and 20-28).

Bethune does not disclose in the sender's apparatus, the light source is for a **linearly** polarized pulse light; a long optical path comprising a half wave plate for rotating the polarization of said signal by 90 degrees; and the optical fiber comprises a single mode optical fiber connected to said first polarized beam splitter, wherein said signal light and said reference light are transmitted through said single mode optical fiber keeping said time delay and said polarization.

However, Bethune discloses that the output from the source laser is preferably horizontally polarized (col 5, lines 6-7). Further, Townsend discloses that the light used in his invention is linearly polarized (col 6, lines1-5). Bethune discloses a long optical path comprising a half wave plate for polarizing light by 45 degrees (Fig 2 and col 5, lines 21-25). Note that the polarization of the signal by 90 degrees appear to be an arbitrary choice on the part of the applicant and it does not patentably distinguish over Bethune's teachings of the half wave plate polarizing by only 45 degrees. The examiner further submits that the use of single mode optical fiber in communication systems was well known at the time the applicant's invention was made. One of ordinary skill would have been motivated to use single mode optical fiber as they result in superior performance when compared to other multi-mode optical fibers, which means that signals can sustain longer transmission lengths before there is a need to regenerate the

signal. Townsend discloses that the optical fiber may be as long as 50 km (col 5, line 56-60), so it is likely that the optical fiber that is used is a signal mode optical fiber. The examiner submits that the above teachings render the above-recited limitations obvious.

Bethune also does not disclose the recipient apparatus comprises a long optical path comprising a half wave plate for rotating the polarization of said reference light and mirrors, and a short optical path comprising a phase modulator for making a phase change for every signal light transmitted through the single mode fiber, wherein the time delay based on the optical path length difference between said short optical path and said long optical path of the recipient's apparatus has the same absolute value and opposite sign to said time delay in the sender's apparatus; a third polarized beam splitter for superimposing said signal light transmitted through the short optical path and said reference light transmitted through the long optical path; and a pair of photoconductor diodes for converting two output lights from said third polarized beam splitter into respective electric signals.

However, Bethune discloses the use of wave plates for polarizing light (col 5, lines 21-25). Further, Townsend discloses two pulse streams traversing paths of unequal lengths (col 4, lines 16-19). Townsend discloses that the two pulses traveling along the unequal length paths are interleaved at another beam splitter (col 4, lines 16-19). Maz discloses the recipient apparatus comprises of a beam splitter for superimposing said signal light transmitted form the sender's apparatus through the other path of transmission and said reference light phase changed by said moveable

mirror of the recipient's apparatus (Fig 4 and col 4, lines 1-14). Maz further discloses the recipient apparatus comprises a pair of photo-detector for converting two output lights from said beam splitter into respective electronic signals (col 3, lines 19-24). These teachings by Bethune, Townsend, and Maz render the above-recited limitations obvious.

Bethune does not disclose:

1. Wherein the sender, by using said movable mirror of the sender's apparatus, randomly imparts phase changes 0, 90, 180, or 270 degrees fro said every signal light, and the recipient, by using said movable mirror of recipient's apparatus, randomly imparts phase change 0 or 90 degrees for said every reference light, as well as measures said difference signal between the electric signals amplified by the charge sensitive amplifier.
2. Then, by using a public communication line, the recipient notifies to the sender said phase changes imparted by the recipient whether it is 0 or 90 degrees for every reference light.
3. The sender calculates the total phase difference between the signal light and the reference light by adding said phase change notified by the recipient and said phase change imparted by the sender for every light, and notifies to the recipient the lights whose total phase difference is either 0 or 180 degrees, as a raw key for candidate being adopted as a privacy key.
4. Then the recipient, for every light notified as a raw key for candidate being adopted as a privacy key, assign bit 1 when said difference signal measured is

equal or greater than a predetermined threshold value +X, and assigns bit 0 when said difference signal measured is equal or less than the predetermined threshold value –X, whereby the recipient gets a privacy key.

5. The sender, for every light making notified as a raw key for candidate being adopted as a privacy key, assigns bit 1 when the phase imparted by the sender is 0 or 90 degrees, and assigns bit 0 when the phase imparted by the sender is 180 or 270 degrees, whereby the sender gets the privacy key.
6. Wherein the sender and the recipient can get the privacy key in common with suitable effective detection efficiency and suitable error rate by selecting said threshold value +X and –X.

However, Townsend discloses a quantum key distribution system wherein a light signal is randomly phase modulated on the sender's end and a recipient to perform a detection of the modulated signal phase shifts the signal again (col 3, lines 26-37). Note the sender phase shifts by 0, $\pi/2$, π, $3\pi/2$ radians and the receiver phase shifts by 0 or $\pi/2$ radians. This is the same as 0, 90, 180, 270 degrees for the sender and 0 and 90 degrees for the recipient. Further, Townsend discloses that after the completion of the quantum communication, the sender and receiver uses a public channel to discuss which photons were encoded and decoded using the same type of phase shift (col 2, lines 9-17 and col 3, lines 55-62). Townsend further discloses that the total phase shift (the sender's phase shift minus the receiver's phase shift) is a used to determine if the key bit of the photon is determined to be a 0 or a 1 (col 3, lines 37-45). Townsend

further discloses that the procedure is completed by comparing the measurements for eavesdropper induced errors (col 3, lines 62-64). These teachings by Townsend read on the above limitations not met by Bethune and Maz.

In light of the above, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Bethune's invention using Maz and Townsend's teachings according to the limitations recited in claim 17. One of ordinary skill would have been motivated to use Maz's teachings because Maz discloses that his teachings would allow for quantum coding by optical phase with a constant delay between the emitter and receiver (col 4, lines 29-34). One of ordinary skill would have been motivated to incorporate Townsend's teachings because Townsend discloses that his teachings would allow one to maintain the quantum cannel effectively over far greater distances than would otherwise be possible (col 2, lines 6-8).

Claim 18:

Bethune discloses a third light polarizes is provided in an output side of said optical fiber for making a correction for a disturbance of polarization of said reference signal (col 5, lines 32-38). Bethune does not disclose said optical fiber is a single mode optical fiber. However, as mentioned, use of single mode optical fiber in communication systems was well known at the time the applicant's invention was made. One of ordinary skill would have been motivated to use single mode optical fiber as they result in superior performance when compared to other multi-mode optical fibers, which means that signals can sustain longer transmission lengths before there is a need to regenerate the signal. Townsend discloses that the optical fiber may be as long as 50

km (col 5, line 56-60), so it is likely that the optical fiber that is used is a signal mode optical fiber.

Claim 19:

Claim 19 recites a limitation substantially similar to what is recited in claim 9. It was discussed in claim 9 how Bethune meets this limitation, thus claim 19 is rejected for the same reasons.

Claim 20:

Claim 20 recites a limitation substantially similar to what is recited in claim 10. It was discussed in claim 10 how Bethune meets this limitation, thus claim 20 is rejected for the same reasons.

Claim 21:

Claim 21 recites a limitation substantially similar to what is recited in claim 11. It was discussed in claim 11 how Bethune meets this limitation, thus claim 21 is rejected for the same reasons.

Claim 24:

Bethune does disclose the signal light has a typical intensity corresponding to a single photon or so, and said reference light has a typical intensity corresponding to photons as large as 10 millions in number. However, this limitation is obvious to the combination invention of Bethune, Maz, and Townsend. Note that Townsend discloses that the quantum channel used is contain at most a single photon per pulse at the source (col 5, liens 9-30). Further, as seen in Figure 4 of Maz, the reference signal (items 130 and 144) is substantially larger than the source signal (items 132 and 140).

The examiner submits that this reads on the limitation that the reference light has a typical intensity corresponding to photons as large as 10 millions in number.

Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bethune et al (US 6,188,768) in view of Mazourenko et al (US 6,272,224), herein referred to as Maz, in further view of Townsend (US 5,675,648) and Bartelt et al (The Wigner Distribution Function—An Alternative Signal Representation in Optics).

Claim 22:

With respect to Claim 22, all the limitations are met by Bethune, Maz, and Townsend except for the following limitation.

The limitation of "characterized in that eavesdropping is detected on the basis of a change in a Wigner distribution function that indicates a quantum mechanical state of said difference signal" is met by Bartelt on page 260.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bartelt the combination invention of Bethune, Maz, and Townsend because the Wigner distribution function is an effective way to determine if the signal has been eavesdropped.

Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bethune et al (US 6,188,768) in view of Mazourenko et al (US 6,272,224), herein referred to as Maz, in further view of Townsend (US 5,675,648) and Lee US 5,665,423).

Claim 23:

As per claim 23, all the limitations are met by Bethune, Maz, and Townsend except the following.

Lee meets the limitation of "characterized in that for said photoconductor diodes, use is made of silicon photoconductor diodes when the light has a wave length of 600 nm to 900 nm, and InGaAs photoconductor diodes when the light has a wave length of 1000 nm to 1500 nm" on column 1, lines 26-38.

It would have been obvious to one of ordinary skill in the art to have modified the combination invention of Bethune, Maz, and Townsend according to the limitations recited in claim 14. One of ordinary skill would have been motivated to do so because the frequency of photodetectors depends on the material used (see Lee, column 1, lines 26-27).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 8:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PP

Primary Examiner
Art Unit 2135